CSDL-AIPS-84-138

ADVANCED INFORMATION PROCESSING SYSTEM (AIPS)

PROOF-OF-CONCEPT SYSTEM

FUNCTIONAL REQUIREMENTS

I/O NETWORK SYSTEM SERVICES

February 28th, 1985

Approved: _____
James E. Kernan, Head, I/O Design Team

Approved: _____
Robert N. O'Donnell, Technical Manager

Approved: _____
Philip G. Felleman, Program Manager

The Charles Stark Draper Laboratory, Inc.
Cambridge, Massachusetts 02139

ACKNOWLEDGEMENT

This report was prepared by The Charles Stark Draper Laboratory, Inc. under Contract NAS9-16023 with the Lyndon B. Johnson Space Center of the National Aeronautics & Space Administration.

A preliminary version of this specification was issued on December 6th, 1984. This revision incorporates changes made to reflect the results of the Phase II Preliminary Design Review held at CSDL on January 23rd - 24th, 1985.

The major contributors were Alan I. Green, James E. Kernan, Alton A. Knosp Jr., Gail A. Nagle, and Gary Schwartz.

Publication of this report does not constitute approval by the NASA/JSC of the findings or conclusions contained herein. It is published for the exchange and stimulation of ideas.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

1.0 GLOSSARY OF I/O NETWORK TERMS

I/O Service Request
Either an request for DIU I/O, a request for Node I/O with contention, or a request for Node I/O without contention.

Node Request Without Contention
A special request for I/O service on exactly one network from the manager of that network consisting of one chained transaction. The individual transactions in the chain involve only nodes; they cannot involve DIUs.

Node Request With Contention
A request for I/O service on exactly one network from the manager of that network consisting of one chained transaction. The individual transactions in the chain involve only nodes; they cannot involve DIUs.

DIU I/O Service Request
A request for I/O service from any user consisting of one or more chained transactions on one or more I/O networks. The individual transactions in the chains involve only DIUs; they cannot involve nodes.

Chained Transaction
A series of one or more transactions on exactly one I/O network.

Transaction
A term that refers to any of the following forms of transactions: input, output, and output/input.

Input Transaction
This type of transaction consists of a command frame followed by a response frame. The predominant information flow is from a node or DIU to a GPC.

Output Transaction
This type of transaction consists of a command frame only. The information flow is from a GPC to a node or DIU.

Output/Input Transaction
This type of transaction consists of a command frame followed by a response frame. There is significant information flow both from the GPC in the command frame and from the DIU or node in the response frame.

Output Transaction with Acknowledgment
This is an output/input transaction in which the data in the response frame contains only the status of the DIU or node.

Frame
A single transmission of data, i.e., a contiguous stream of bits from the opening to the closing flags inclusive.

Command Frame
A frame transmitted by a GPC on an I/O network resulting in the transmission of an output packet.

Response Frame
A frame transmitted by a node or a DIU on an I/O network in response to a received command frame, resulting in the receipt of an input packet by a GPC.

Input Packet
The collected information resulting from a response frame.

Output Packet
The total information transmitted by a command frame.

Contention Sequence
The modified Laning Poll that is performed on a network in order to permit the GPC to perform a chained transaction.

Laning Poll
A contention resolution scheme based on relative priority.

DIU
A Device Interface Unit that interfaces the network to sensors, effectors, and other I/O devices.

Subscriber
A GPC or a DIU connected to a network.

Link
A full duplex, serial transmission path.

Net Link
A link connecting two nodes.

Root Link
A link connecting a GPC to a node.

DIU Link
A link connecting a DIU to a node.

Node

A unit of equipment. that steers transmissions between nodes or between nodes and subscribers

I/O Network

A fault-tolerant, reconfigurable connection between subscribers. The network is made up a number of 5-ported circuit switched nodes. The nodes are interconnected via net links. Subscribers are connected to the network via root links (GPCs) and DIU links.

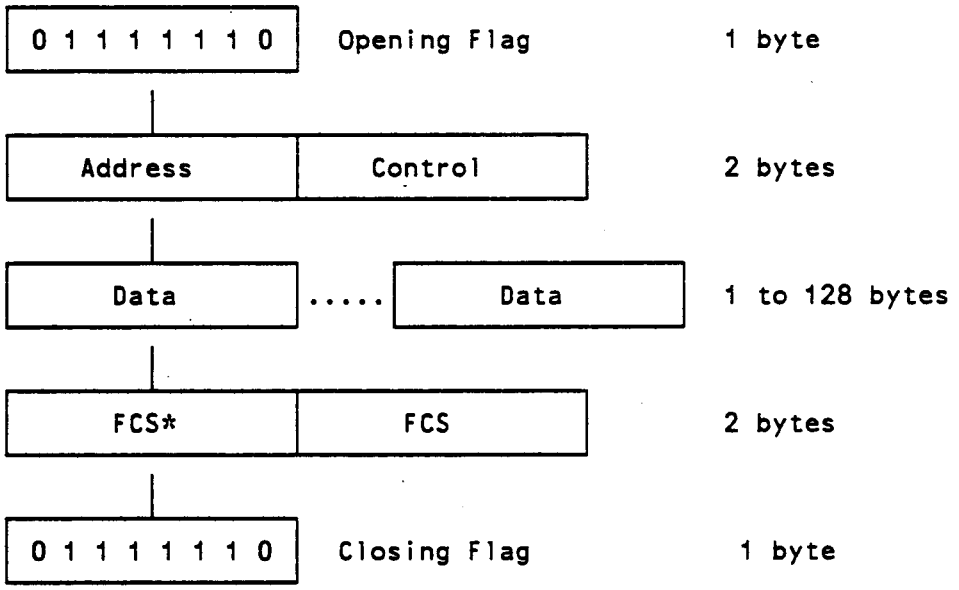
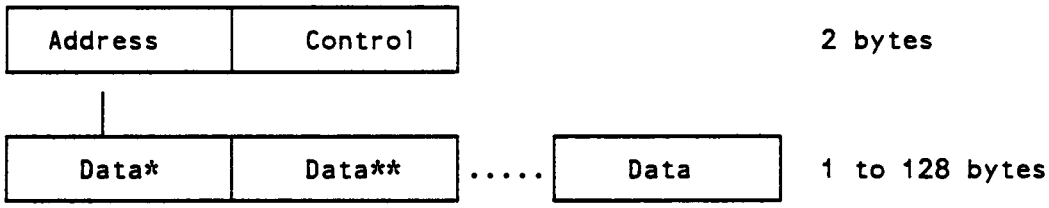


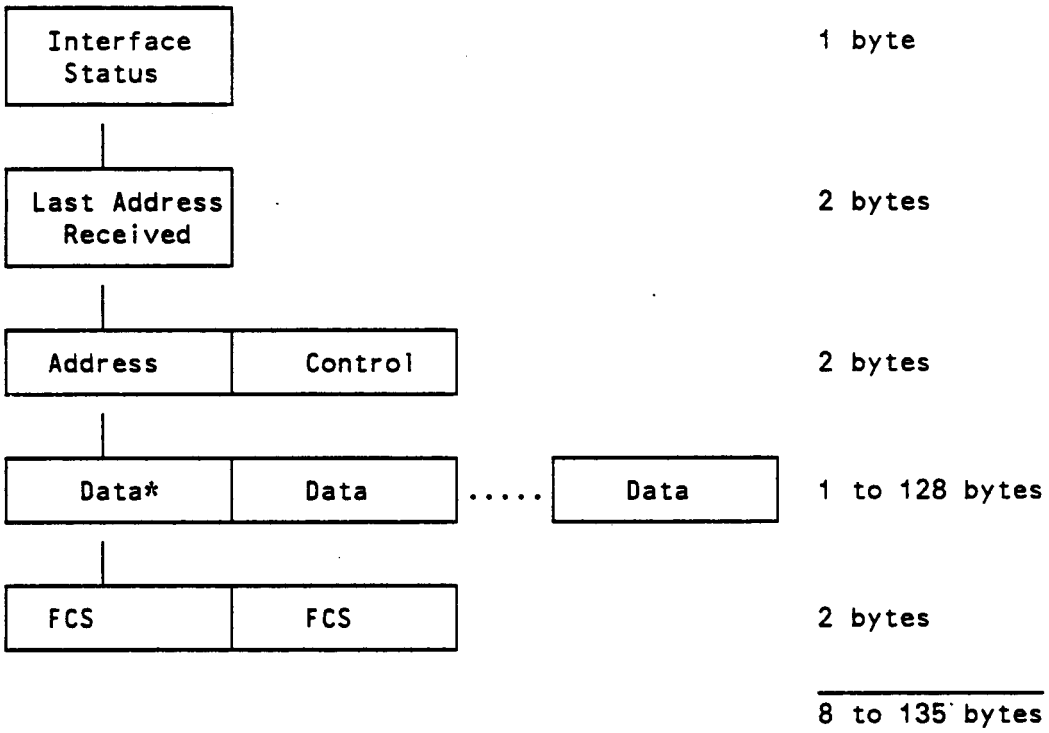
Figure 1. Frame Format



* For an output packet addressed to a DIU, the one's complement of the DIU address will be contained in the first byte of the data field.

** For an output packet addressed to a DIU, the subcontrol information followed by its one's complement will begin in the second byte of the data field. The exact number of bytes of subcontrol information is DIU specific.

Figure 2. Output Packet Format



* For an input packet from a DIU, the first byte of the data field will contain the one's complement of the DIU address.

Figure 3. Input Packet Format

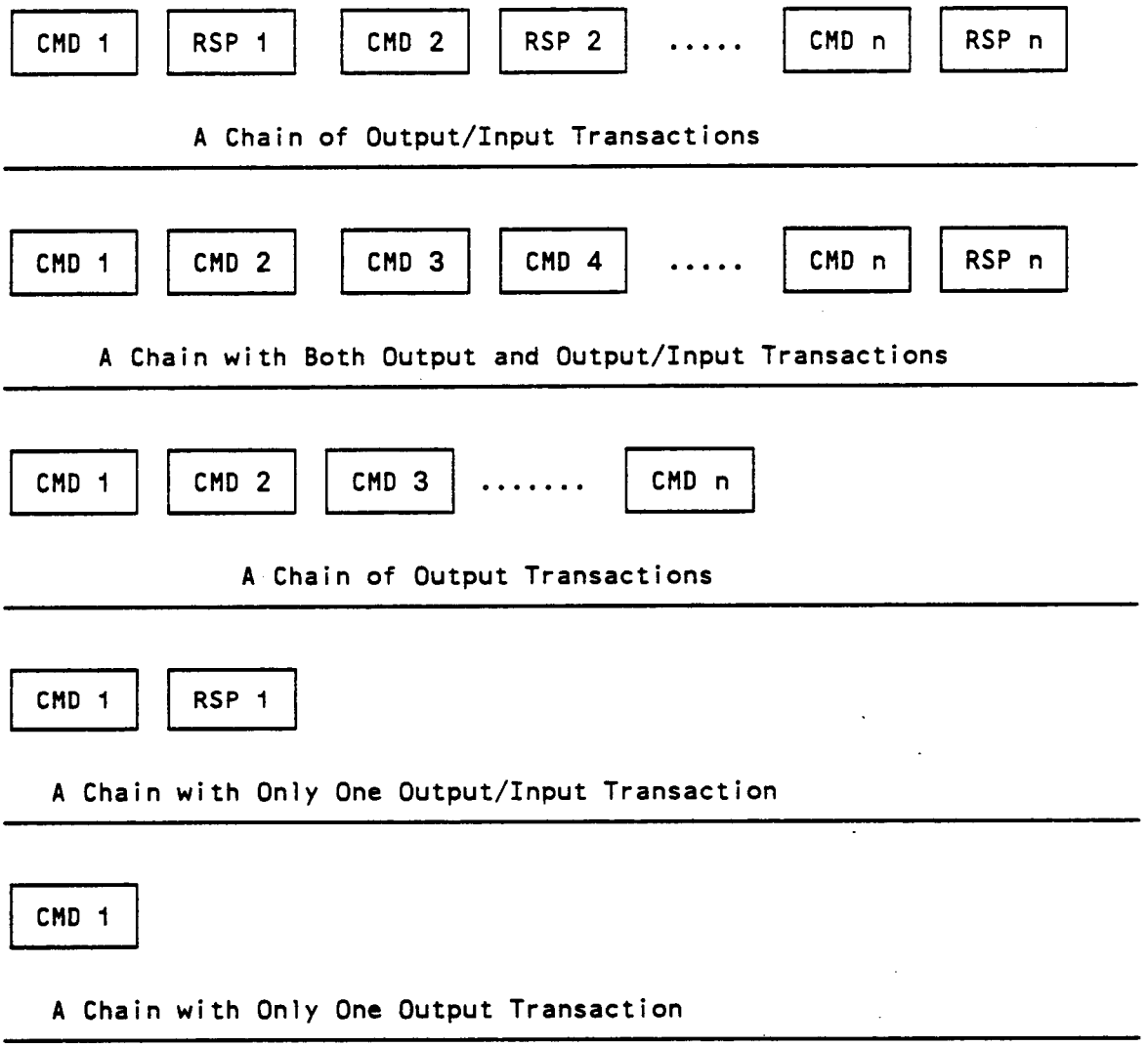


Figure 4. Chained Transactions

2.0 GENERAL I/O REQUIREMENTS

The I/O system within each GPC shall support the capability of performing concurrent operations on all I/O networks to which the GPC is connected.

Within each GPC, multiple I/O Service Requests shall be processed concurrently to the extent possible. The limitation is that overlapped use of the same I/O network by different chained transactions is not supported. Any chained transaction that attempts to use an I/O network not currently in use will be started without delay; whereas a chained transaction for an I/O network already in use will be delayed.

It shall be possible to continue the performance of I/O for an Application Function concurrently with the migration of an unassociated Application Function.

The I/O system software shall not perform flow control of the I/O data. That is, the application software design must account for flow control (perhaps by not requesting an I/O Service Request again until the previously one has been processed).

3.0 I/O USER COMMUNICATION REQUIREMENTS

I/O System Services must provide two general categories of I/O User Communication Services. The first category covers requests for the transfer of data between a GPC and some I/O device external to the GPC. These requirements are contained in "3.1 I/O Service Requests." The second category covers capabilities for modifying certain characteristics of I/O Services. The requirements for this second category are contained in "3.3 Miscellaneous Services" on page 13.

3.1 I/O SERVICE REQUESTS

Requests for I/O service consist of three distinct types: Network Node I/O Requests that do not involve a contention sequence, Network Node I/O Requests that do involve a contention sequence, and DIU I/O Requests.

3.1.1 Node Requests without Contention

I/O service requests that are addressed to nodes and that omit the network contention protocol can be requested only by the Network Control and Management function within the GPC that is the current manager of the network. No other function shall be permitted to initiate this type of I/O.

3.1.1.1 Scope

An I/O Request of this type can involve only a single network. In this context, a network is either a global, regional, or local I/O network.

The transactions in this type of I/O Request can be addressed only to nodes; they cannot be addressed to DIUs.

3.1.1.2 Inputs and Outputs

It shall be possible to perform both input and output transactions in this type of I/O Request.

3.1.2 Node Requests with Contention

I/O service requests that are addressed to nodes and that do not omit the network contention protocol can be requested only by the Network Control and Management function within the GPC that is the current manager of the network. No other function shall be permitted to initiate this type of I/O.

3.1.2.1 Scope

An I/O Request of this type can involve only a single network. In this context, a network is either a global, regional, or local I/O network.

The transactions in this type of I/O Request can be addressed only to nodes; they cannot be addressed to DIUs.

3.1.2.2 Inputs and Outputs

It shall be possible to perform both input and output transactions in this type of I/O Request.

3.1.3 DIU I/O Service Requests

DIU I/O Requests can be requested by any user.

3.1.3.1 Scope

A single DIU I/O Request can involve any number of I/O networks. In this context, an I/O network is either a global, regional, or local I/O network.

The transactions in this type of I/O Request can be addressed only to DIUs; they cannot be addressed to nodes.

3.1.3.2 Inputs and Outputs

It shall be possible to perform both input and output transactions in this type of I/O Request.

3.1.4 Service Request Processing

3.1.4.1 Request Priority

Within each GPC, the chained transactions on each network shall be performed on a priority basis.

All chained transactions of a particular Service Request will have the same priority. As a class, Node Requests without Contention shall have priority over both other kinds. The relative priorities of Node Requests with Contention and DIU I/O Service Requests shall be decided by the design process.

3.1.4.2 Chained Transactions

Each I/O Service Request shall be organized such that all the transactions concerned with any one network are contained in a single chained transaction, i.e., there is a limit of one chain per network per I/O Request. Each chained transaction shall be initiated separately and independently from any other chains on other networks.

Chained transactions shall be predefined. However, the user can specify a particular subset of the individual transactions in a predefined chain (see "3.3.2 Transaction Selection" on page 13). In addition, individual transactions can be bypassed in response to errors.

3.1.4.3 Transactions

A transaction is a single 'conversation' with a node or a DIU. It consists of one or two frames depending on whether it is a simple output transaction (one frame), or an output/input transaction or an input transaction (two frames).

The source and destination addresses for output and input packets respectively shall be under software control.

3.1.4.4 Service Request Options

3.1.4.4.1 WAIT FOR COMPLETION

It is required that the user have the option of either waiting or not waiting for the I/O Service Request to complete before the user's processing is allowed to continue.

If the wait option is selected the requesting user's processing will be suspended until all portions of the I/O Service Request have been completed. The requester has the responsibility of performing any desired timeout in this option.

If the wait option is not selected the requesting user's processing will be allowed to continue in parallel with the servicing of the I/O Service Request (subject, of course, to the other factors that control the multiprogrammed GPC). If the wait option is not selected the I/O Service Request processing software shall set an indicator when each chained transaction of the Service Request completes. The requesting user must interrogate these indicators before initiating processing related to the data collected by the chained transaction, in order to avoid the use of incoherent data.

3.1.4.4.2 NO TRANSACTION BYPASS

It is required that the user have the option to disable the transaction bypass feature of the I/O error processing software. If this option is selected the I/O error processing software shall discontinue logging the occurrence of errors associated with this transaction when the normal bypass threshold has been exceeded. This error logging shall be reenabled if the transaction completes without error.

This option should only be used for transactions that are addressed to DIUs for which an independent on/off indication is not available. In this case, attempting I/O is the only way to detect that the DIU has been activated. The aspect of this feature that discontinues the error log entries prevents the saturation of the error logs when such a DIU is off for an extended period.

This feature should only be selected for a transaction if that transaction is the only transaction in a chain. (This restriction is imposed to prevent delayed responses by the nonbypassed DIU from causing errors in subsequent transaction(s) in the chain.)

3.1.5 Separation of I/O Service Requests

Each Service Request shall be treated as a separate entity. The implementation shall not combine transactions related to one Service Request with those related to another to create nonpredefined chained transactions. Neither shall the implementation attempt to optimize the network utilization by not performing redundant transactions in either the same or different Service Requests.

3.2 FAULT PROTECTION AND NOTIFICATION

I/O Request Servicing shall protect the user from faults that interfere with I/O communications.

3.2.1 Transaction Bypass

The I/O Service Request processing shall protect the system from excessive overhead that would be caused by the processing of recurring errors. This will be accomplished by bypassing (not performing) a transaction that has experienced a communication error for two consecutive occurrences of the Service Request. The requesting user shall be supplied with an indication that a transaction bypass has or has not been performed.

The switching of root links is discussed in "4.1.1.2 Error Response" on page 15. The bypassing of transactions and the switching of root links are exclusive actions. If the conditions are met that dictate that a root node switch should be performed, that action shall take precedence over transaction bypass.

If multiple transactions reach the criterion for bypass on the same occurrence of the chained transaction, only the first of these transactions in the chain shall be bypassed. The remaining transactions shall not be bypassed until subsequent occurrences of the chained transaction, and then only if the transactions experience errors again. The rule is: only one transaction bypass per occurrence of a chained transaction - the first errored transaction in the chain.

If the chained transaction is being performed on a partitioned network, the bypassed transaction shall be replaced with a time pad equivalent to the duration of the bypassed transaction. The purpose of inserting a time pad is to maintain the simultaneity of transactions on the different partitions of the network.

For the clearing of transaction bypass see "3.3.3 Transaction Bypass Clearing" on page 13.

3.2.2 Communication Fault Indication

The requesting user shall be supplied with an indication that a communication error has occurred, since this invalidates the received or transmitted information. There shall be a separate indication for each transaction within a chained transaction. Every transaction in the chain that experienced an error shall have its indicator set. Conversely, every transaction in the chain that occurs without an error shall have its indicator cleared. For bypassed transactions, the Communication Fault Indicator shall remain set for the duration of the bypass.

3.3 MISCELLANEOUS SERVICES

This section covers the second category of I/O User Communication Services: capabilities for modifying certain characteristics of I/O Services.

3.3.1 I/O Service Request Initialization

Upon GPC turn on the System Software I/O Service Requests shall be initialized.

It shall be possible to command the initialization of all of an Application Function's I/O Service Requests.

3.3.2 Transaction Selection

It shall be possible for the user to specify a particular subset of the individual transactions in a predefined chain. This specification will be in effect until a different Transaction Selection is invoked. However, the actual execution of an individual transaction also depends on its bypass state. When Transaction Selection is invoked to select a transaction, the bypass state of the transaction shall be cleared.

3.3.3 Transaction Bypass Clearing

Following a network repair operation, the bypass state of all transactions associated with active Application Functions will be marked for clearing. Similarly, the bypass state of transactions within System Software I/O Service Requests shall also be marked for clearing following a network repair operation. The actual clearing will take effect upon the next occurrence of the I/O Service Request.

It shall also be possible to mark all chained transactions associated with a particular Application Function for clearing of their transaction bypass states upon the next occurrence of the chain. This operation would be performed in conjunction with a function migration and perhaps following a network repartition.

The operation of bypass state clearing shall cause the clearing of all error counters and indicators associated with the restored transaction, including its Communication Fault Indicator.

4.0 NETWORK CONTROL REQUIREMENTS

4.1 LOCAL GPC CONTROL REQUIREMENTS

4.1.1 Functions

4.1.1.1 Subscriber Link Control

Each GPC shall control the state of its ends of all its subscriber links.

Only one subscriber link to a particular network or network partition shall be active at any one time.

4.1.1.2 Error Response

If a GPC has more than one link to a network or network partition it shall continue to use the currently active link until it encounters errors that indicate an inability to communicate with the network via the currently active link. Then it shall switch to an alternate link. If all links to a particular network or network partition are failed the GPC shall log a failure report for the System Function Migration Manager.

4.1.2 Performance

The length of time to switch to an alternate link to a network or network partition should be kept as small as practical in order to hold to a practical minimum the length of time that the network is out of service to the GPC's users.

4.2 MANAGER GPC CONTROL REQUIREMENTS

4.2.1 Functions

4.2.1.1 Initialization

When the network is initialized, all nodes and ports shall be declared nonfailed and the network shall be regrown from a single root link of the network manager GPC. However, if the network is partitioned, each partition shall be grown from a separate root link.

4.2.1.2 Network Definition

It shall be possible to partition a network into a number of subnetworks. The number of possible partitions shall be no more than the number of links that the network manager GPC has to the network in

question. The network manager will alter the network partitioning only upon the occurrence of a 'redefinition' event. In this context, a 'redefinition' event is either a migration of the network manager in question, a system reconfiguration that assigns a new set of functions to the GPCs that are subscribers on the network, or a network failure that would otherwise result in the isolation of a DIU. The network reconfiguration operations that are performed between these partition redefinition events shall not employ the links that would interconnect the partitions.

The partitioning of a network into subnets shall only be permitted if the manager GPC is the sole user of all partitions.

4.2.1.3 Network Monitor

4.2.1.3.1 NODE MONITOR

The network manager shall periodically collect the status of all the nodes of the network. Any errors experienced while attempting to collect the node status information shall be used to determine the proper reconfiguration action. In the absence of any of the aforementioned errors, the node status information itself shall be used to determine the proper reconfiguration action.

4.2.1.3.2 GPC SUBSCRIBER MONITOR

The network manager shall periodically collect the status of all GPC subscribers of the network. This status shall be limited to that information which is germane to the use of the network by the GPC. This information shall be used to maintain the I/O Network status log (see "5.2.2 Status Collection" on page 19).

4.2.1.4 Network Maintenance

Under nonfailure conditions, the network shall be maintained such that all subscribers are interconnected via active links. Under failure conditions, the network shall be maintained such that as many subscribers as possible are interconnected via active links.

All node ports that are part of GPC root links shall be maintained active so as to permit the GPC to locally control its active root link to the network.

4.2.1.5 Spare Testing

Nonfailed spare links shall be periodically tested for functionality. This should be done in order to purge faulty nodes and links from the pool of resources.

4.2.2 Performance

The length of time that the network is out of service due to reconfiguration operations should be held to a practical minimum.

5.0 STATUS LOGGING, COLLECTION AND REPORTING REQUIREMENTS

The duties related to the logging, collecting, and reporting of status information pertaining to each I/O network shall be shared by the GPCs that are subscribers on the network, the GPC that is the manager of the network, and the Global GPC. The intent of this sharing is that the manager and Global GPCs should manage only that information that they require for the performance of their functions. It is not intended that all information be duplicated at each level: subscriber, manager, and global. The relationship among these three levels is depicted in Figure 5. The information flow between levels may be nil in some cases.

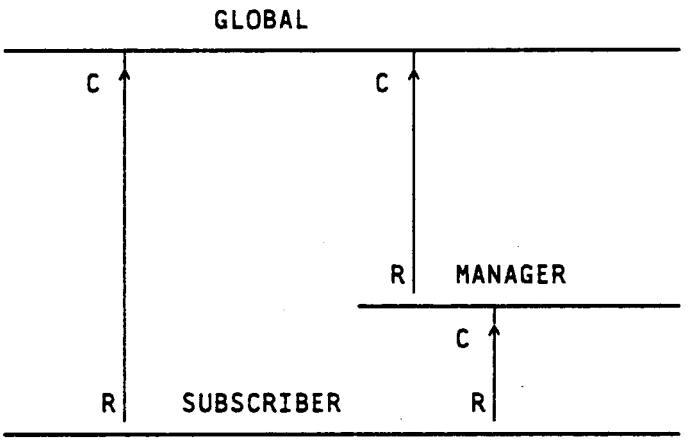


FIGURE 5. STATUS COLLECTION (C) AND REPORTING (R) LEVELS

The implementation should take care that these requirements do not consume an excessive amount of resources. For example, the error and configuration logs should either be maintained on a mass storage medium or in a circular log within the GPC.

5.1 SUBSCRIBER GPC REQUIREMENTS

5.1.1 Status Logging

5.1.1.1 Error Logging

Each GPC shall maintain a log of I/O errors detected by that GPC. Sufficient information should be included in the log so as to be able to identify the type and time of the error.

5.1.1.2 Configuration Logging

Each GPC shall maintain a log of I/O configuration changes performed by that GPC. Sufficient information should be included in the log so as to be able to identify the type and time of the configuration change. The types shall include software as well as hardware configuration changes.

5.1.2 Status Reporting

5.1.2.1 Error Reporting

Each GPC shall report its I/O error information to the appropriate manager or global GPC. The information reported shall be limited to that which is needed for network management.

Each GPC shall report I/O error information to the Global Computer. This information shall be limited to that which pertains to a possible need for function migration.

The stimuli for performing the reporting functions shall be decided by the design process.

5.1.2.2 Configuration Reporting

Each GPC shall report its I/O configuration information to the appropriate manager or global GPC. The stimuli for performing the reporting functions shall be decided by the design process.

5.2 MANAGER GPC REQUIREMENTS

The manager of an I/O network shall maintain a log of information pertaining to the network.

5.2.1 Status Logging

5.2.1.1 Error Logging

The manager GPC shall log the collected node status information that leads to network configuration changes. Any errors detected during the reads of the nodes to acquire status information will be included in the subscriber GPC information for the GPC that performs the network manager function.

5.2.1.2 Configuration Logging

All network configuration changes shall be logged.

5.2.2 Status Collection

5.2.2.1 Error Collection

Information concerning the errors detected by each subscriber GPC shall be periodically collected from same so that a single log of all errors detected on the network is centrally maintained. The information collected should be limited to that which allows traceability to the detailed information contained in the subscriber GPC error log (see "5.1.1.1 Error Logging" on page 17).

5.2.2.2 Configuration Collection

The network manager shall collect appropriate I/O configuration information from the GPC subscribers.

5.2.3 Status Reporting

The status information reported by the manager GPC to the Global GPC shall be limited to that which is required to perform system wide reconfiguration decisions such as function migration.

5.2.3.1 Error Reporting

The manager GPC shall report appropriate error information to the Global GPC. The information shall be limited to that pertinent to the network manager's ability to continue. The stimulus for performing the reporting function shall be decided by the design process.

5.2.3.2 Configuration Reporting

There is no requirement to report I/O network configuration information to the Global Computer.

5.3 GLOBAL GPC REQUIREMENTS

The Global GPC shall collect status information from each GPC that is a functioning subscriber on an I/O network. This shall include error and configuration information pertaining to the manager GPC and the other GPCs that are subscribers on the I/O network. This information should be limited to that which is needed by the Global GPC in order for it to perform its system wide configuration management functions.

6.0 TEST SUPPORT REQUIREMENTS

6.1 GENERAL

The requirements in this section are of a general nature. The first grouping below relates to practices that should be followed as the I/O software is developed.

Key I/O software control variables shall be alterable so as to assist testing and experimentation.

Significant I/O software variables shall be declared so that they are permanent (static). The intention is to avoid reassigning the storage locations for these variables before they are externally observable for test purposes.

The following grouping relates to test activity recording capabilities. The first two items are not unique to I/O testing; they are expected to be necessary for general use in all areas of testing.

The capability shall exist to trace selected portions of software execution.

The capability shall exist to dump selected portions of GPC memory to a permanent storage medium.

The capability shall exist to record an indication of every transaction that occurs on a network in the order of occurrence.

The requirements of section "5.0 Status Logging, Collection and Reporting Requirements"themselves support testing because they provide for a chronological record of I/O related configuration change and error events.

6.2 I/O NETWORK MODIFICATIONS

These requirements relate to the condition of an I/O Network to support different test situations.

It shall be possible to modify the physical connections of links to nodes in order to obtain different networks. It shall also be possible during testing to order via external command that the software modify its definition of an I/O network for the purpose of conforming with the actual network.

It shall be possible during testing to order via external command the use of a different partitioning of an I/O network.

6.3 FAULT AND ERROR INJECTION

This section contains requirements related to causing various kinds of faulty and erroneous I/O behavior.

The mechanisms that cause the occurrence of various faulty and erroneous behavior shall be capable of being coordinated by an external programmable test coordinator.

It shall be possible during testing to order via external command the clearing of bypassed transactions.

It shall be possible to cause a transmission error in any transaction or combination of transactions in a chain. Both one occurrence of a chain and every occurrence of a chain options shall be available.

It shall be possible to set the contents of any field or combination of fields of an input packet to particular arbitrary values (normal or abnormal). Both one occurrence and every occurrence options shall be available.

It shall be possible to set the contents of any field or combination of fields of an output packet to particular arbitrary values (normal or abnormal). Both one occurrence and every occurrence options shall be available.

It shall be possible to cause the response frame for any command frame not to occur. Both one occurrence and every occurrence options shall be available.

It shall be possible to cause any network link to fail open.

It shall be possible to inject stuck-at faults (both one and zero) at the receive and transmit terminals of a node port.

It shall be possible to cause a selected node to behave erratically. Options shall be available for both sporadic (occasional) and continuous transmission uncorrelated with other network activity.

It shall be possible to cause a node to respond to various addresses: its true address, a different address, all addresses, and no address.

It shall be possible to cause a DIU to respond to various addresses: its true address, a different address, all addresses, and no address.

It shall be possible to cause a selected GPC to transmit erratically. Options shall be available for both sporadic (occasional) and continuous transmission uncorrelated with other network activity by other GPCs.

It shall be possible to cause any I/O channel or combination of I/O channels in a GPC to be unable to win a contention on an I/O network.

7.0 IOP-IOS FUNCTIONAL INTERFACE REQUIREMENTS

This section contains a description of the functional interface requirements between the IOP and the IOS for the Proof of Concept System.

The IOS is a component of the I/O interface whose purpose is to relieve the IOP of the burden of loading (sequencing) a chain of transactions from memory to the I/O interface. It also relieves the IOP of the necessity of processing transactions, I/O status, and error information in real time as they are delivered by the I/O interface. To accomplish this, the IOP and IOS communicate via a dual port memory (DPM). There is one DPM per IOS.

7.1 IOP-IOS DPM INTERFACE PARAMETERS

Every IOP must communicate three control parameters to its selected IOS (i.e., its IOS within the interface for the chain's network). These parameters are read by the IOS from its DPM to determine:

1. When a chain of transactions needs to be processed
2. The dual port memory address of the chain of transactions
3. The dual port memory address of the DIU/Node Partition Information

The first of these parameters is described in section "7.1.1 Chain-to-Process Indicator" below. The second points to the data which describes the chain. This data is described in section "7.1.2 Chain Description Data." The third parameter points to the table defining which of the I/O interfaces connecting the GPC to the network may be used to communicate with specific DIUs or nodes. This table is used when the network is divided into more than one partition; it is described in section "7.1.3 DIU/Node Partition Information."

7.1.1 Chain-to-Process Indicator

This indicator is a signal to the IOS that there is a chain to be processed. There is only one of these indicators per IOS and there is no priority or interruption requirement.

7.1.2 Chain Description Data

This information is made accessible by the address of the chain (the second of the IOP-IOS control parameters). It includes information common to the chain of transactions as a whole, as well as information relevant to the individual transactions.

7.1.2.1 Chain Header Data

The chain header data describes the chain of transactions as a whole. It also provides access to information relevant to each individual transaction, and also to the End-of-Chain (EOC) status information. Specifically, it includes:

1. The programming necessary to initialize the HDLC chip to send frames to either nodes or subscriber sites

2. The dual port memory address of the transaction description data for the first transaction in the chain

3. The dual port memory address of the EOC status indicators

4. The maximum time before the chain should be declared ended due to a time-out (this may, perhaps, default to the maximum allotted bus time for a transaction)

5. Whether or not the chain must win the network contention before beginning transmission

6. The priority to be used for the initial contention for the network, if contention is required.

EOC status is modifiable in real time and only by the system (not the application).

7.1.2.1.1 TRANSACTION DESCRIPTION DATA

The transaction description data contains information corresponding to each transaction. It should specify:

1. User transaction selection

2. Transaction bypass disable

3. Transaction bypass

4. Transaction error count

5. The I/O Network address of the destination

6. The HDLC control byte

7. The dual port memory address of the data to be sent in an output packet

8. The length of the data to be transmitted

9. A time pad value which may optionally be used to replace the transaction when the transaction is bypassed (used to coordinate the timing of transactions within a chain)

10. An indication of whether or not an input frame is expected in response to the output frame

11. The dual port memory address where the input packet resulting from the response frame (if expected) should be stored

12. The expected length of the input packet

13. The time-out value to be used to determine when the response has been "completed" due to a failure

14. The dual port memory address of the next transaction in the chain, if it exists

User transaction selection, transaction bypass, output packet data, and input packets are modifiable in real time. Output packet data and user transaction selection are modifiable by the application. Transaction bypass and input packets are modifiable only by the system.

7.1.2.1.1.1 OUTPUT PACKET DATA

The storage allocated for the output packet contains data values provided by the requester of the transaction.

7.1.2.1.1.2 INPUT PACKET

The input packet, created by the IOS, should contain the following information:

1. Interface Status (IFS), consisting of indicators for:
   - transaction time-out
   - incorrect message length
   - frame protocol error (CRC, invalid frame, or abort)
2. Number of bytes received
3. An indication of whether or not the network address in the response frame from a DIU matched the network address in the corresponding command frame
4. HDLC control byte specified in the response frame
5. Data from the response frame
6. FCS from the response frame

7.1.2.1.2 EOC STATUS INDICATORS

The EOC status is comprised of indicators that are set by the IOS to reflect the post execution health of the chain as a whole, or in some cases, why the chain was unable to run. Specifically, they are:

1. Chain time-out

2. Network line busy

3. Poll failure (poll not won within maximum number of attempts)

4. Poll abort detected

5. The occurrence of a transaction time-out or frame protocol error or incorrect message length in one or more transactions within the chain

6. Indication that all transactions had an error

7. Indication if response frames from more than one DIU were expected

7.1.3 DIU/Node Partition Information

This information is made accessible by the address of the DIU/Node Partition Information (the third of the IOP-IOS control parameters). It must specify:

1. The DIU and node addresses accessible by the network

2. Which DIUs and nodes are accessible from each IOS for the current partitioning of the network

This information shall be used by a given IOS to automatically skip transactions directed to DIUs or nodes that are not accessible to the IOS due to the current partitioning of the network. Each IOS that connects a GPC to a particular I/O network must have a unique ID. The following figure depicts this information.

DIU/Node	IOS 1 Connected	IOS 2 Connected	IOS 3 Connected
Address	yes/no	yes/no	yes/no
Address	yes/no	yes/no	yes/no
Address	yes/no	yes/no	yes/no
. .	. .	. .	. .

Figure 6. DIU/Node Partition Association Information

8.0 DIU FUNCTIONAL INTERFACE REQUIREMENTS

This section contains a description of the functional interface requirements of a Device Interface Unit (DIU) for the Proof of Concept System.

These requirements are consistent with the intended design of the GPC I/O software in that during any one contention sequence to contention sequence interval, only one GPC will have its receive DMA path enabled.

8.1 HDLC PROTOCOL

A DIU must conform to the protocol of an I/O Network - HDLC.

For the Proof of Concept system, the nomenclature that applies to HDLC frames is: a frame that is transmitted by a GPC subscriber on an I/O Network is a Command Frame, a frame that is transmitted by an DIU is a Response Frame.

8.1.1 Command Frame

8.1.1.1 Address Field

The DIU must recognize its address in a Command Frame that is transmitted by another subscriber on the network.

8.1.1.2 Control Field

There are no present plans to utilize the control field. The DIU shall ignore its contents.

8.1.1.3 Data Field

The data field will contain:

1. a redundant version of the address in some encoded form
2. some number of bytes of subcontrol information
3. optionally, an additional number of bytes of data content

The total number of bytes in a data field is limited to 128.

8.1.1.3.1 REDUNDANT ADDRESS

A DIU shall check the redundant version of the address with respect to the value contained in the address field. If the two versions are not equivalent the DIU shall:

- record the occurrence of an error in its status storage
- not perform the command

8.1.1.3.2 SUBCONTROL INFORMATION

The subcontrol information will inform the DIU of the specific nature of the requested action. For example, it will indicate whether or not a response is involved. The subcontrol information will also indicate to the DIU which devices (if any) are involved in the requested action.

The subcontrol information will be encoded so as to prevent a single fault from modifying the subcontrol information so that it looks like a different valid value. The DIU shall respond to only valid subcontrol information. If the subcontrol information is not valid the DIU shall:

- record the occurrence of an error in its status storage
- not perform the command

8.1.1.3.3 DATA CONTENT

The DIU shall distribute the data content portion of the data field (if any) to the destination(s) indicated by the subcontrol information. There is no system level encoding of the data content.

8.1.1.4 Frame Check Sequence

A DIU must verify the validity of the FCS in a Command Frame. If the FCS is invalid the DIU shall:

- record the occurrence of an error in its status storage
- not perform the command

8.1.2 Response Frame

A DIU will transmit a Response Frame if the subcontrol information in the Command Frame so indicates.

8.1.2.1 Address Field

A DIU shall return its own address in the Response Frame Address Field. (This is preferred, for safety reasons, to the alternative of returning the address of the transmitting GPC. The nonpreferred alternative would imply that all GPCs are ready to receive the DIU transmission and therefore a faulty DIU could pollute a GPC that was not the intended destination of the transmission.)

8.1.2.2 Control Field

There are no present plans to utilize the control field. It must, of course, be present, so the DIU must fill it with something - any value is acceptable.

8.1.2.3 Data Field

The data field will contain:

1. a redundant version of the DIU address in some encoded form
2. optionally, some number of bytes of data content. The exact number depends upon the action requested by the subcontrol information in the Command Frame.

The total number of bytes in a data field is limited to 128.

8.1.2.3.1 REDUNDANT ADDRESS

The DIU shall generate a redundant version of its address for inclusion in the data field. The redundant version of the address shall be in some encoded form. The specifics of the encoding shall be identical to those used for the redundant address in the Command Frame. The mechanization shall ensure that the address value in the address field and its redundant form in the data field are not subject to compensating errors from a single fault.

8.1.2.3.2 DATA CONTENT

The DIU shall collect the data for the data content portion of the data field (if any) from the source(s) indicated by the subcontrol information in the Command Frame. There is no system level encoding of the data content.

8.1.2.4 Frame Check Sequence

A valid Frame Check Sequence must be generated for each frame the DIU transmits.

8.2 DIU STATUS INFORMATION

The DIU shall record, in its status storage, a separate indication of errors it perceives related to address, subcontrol information, and FCS.

Every DIU shall be capable of transmitting a Response Frame that contains the status of the DIU. The status information contained in the storage shall be reinitialized after being transmitted.

8.3 COMMAND FRAME - RESPONSE FRAME RELATIONSHIPS

For every Command Frame there is either exactly one Response Frame or exactly none. The subcontrol information in the Command Frame will indicate which response is expected.

The DIU shall distribute any additional data bytes that follow the subcontrol information in a Command Frame to the destination(s) indicated by the subcontrol information.

If a Response Frame is called for, the DIU shall collect the data from the source(s) indicated by the subcontrol information.

8.4 ADDRESS AND SUBCONTROL INFORMATION ENCODING

8.4.1 Redundant Address

The redundant form of the address contained in the data field of Command and Response Frames shall be the ones complement of the DIU address. For Response Frames, the DIU shall generate the complement form from a source other than the value received in the Command Frame. For both Command and Response Frames, the redundant address shall be contained in the first byte of the data field.

8.4.2 Subcontrol Information

The subcontrol information received in the data field of a Command Frame shall be encoded in true/complement form. The ones complement shall be used. The subcontrol information, including both true and complement form, shall begin in byte 2 of the data field of a Command Frame. The exact number of bytes of subcontrol information is DIU specific.